

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Rachel S. Corn, a Special Agent (SA) with the Federal Bureau of Investigation (FBI),
Baltimore Division, Baltimore, Maryland, being duly sworn, depose and state as follows:

1. I have been a SA with the FBI since May 2006. Since September 2006, I have primarily investigated federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received FBI Crimes Against Children training, FBI Innocent Images Online Undercover training, and FBI Peer-to-Peer Network Online Investigation training. I have participated in the execution of numerous search warrants, of which the majority have involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United States Code § 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with the FBI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a warrant to search the following (hereinafter referred to as the “TARGET LOCATIONS,” more fully described in Attachments A1 and A2, incorporated here by reference):

a. The associated files of Cybertipline Report 2194409 that was forwarded to the National Center for Missing and Exploited Children (NCMEC) by GoDaddy.com/Wild West Domains; and

b. The GoDaddy.com website <http://avza.berydoq.com> to include the Sub-Domain Names set up on berydoq.com: avza.berydoq.com, blzy.berydoq.com, cuyo.berydoq.com, dalj.berydoq.com, and associated with customer account: Steven Bickling, 3514 Elliott, Baltimore, MD 21224 Phone: 4437397509, bick36@gmail.com.

4. The TARGET LOCATIONS is to be searched for evidence of violations of Title 18, United States Code, Sections 2251(a) (sexual exploitation of children); Title 18, Section 2422(b) (attempted online coercion and enticement of a minor); Title 18, United States Code, Section 2252A(a)(2) (distribution and receipt of child pornography); and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) (the “TARGET OFFENSES”).

5. The statements in this affidavit are based in part on information and reports provided by the Baltimore City Police Department and Special Agents of the FBI, on my investigation of this matter, and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES are located in the TARGET LOCATIONS.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had

discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

7. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

h. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET LOCATIONS notwithstanding the passage of time.

j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

k. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

l. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

n. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

NCMEC CYBERTIPLINE

8. The National Center for Missing and Exploited Children (NCMEC) receives complaints via their Cybertipline from Internet Service Providers (ISPs), Electronic Service Providers (ESPs), and others. These Cybertipline reports are reviewed by a NCMEC analyst and forwarded to law enforcement for further investigation on the information provided in the Cybertipline report.

PROBABLE CAUSE

9. On May 21, 2020, an online tip was submitted to the FBI National Threat Operations Center (NTOC), via the website tips.fbi.gov, to report allegations involving an individual viewing videos depicting minors getting sexually abused. Follow up investigation determined that Steven Bickling (“Bickling”), residing at 27 South Curley Street, Baltimore, Maryland 21224, was the subject of the online tip.

10. In 2014, Yahoo, Inc., conducted an internal investigation of Yahoo users selling and buying suspected child abuse images, videos, and live-streams located in the Philippines. During this investigation, Yahoo identified hundreds of potential sellers and buyers of the suspected child pornography files. One buyer was identified by Yahoo as:

Yahoo ID:	apoc39
Name:	Steve Bickling
Location:	Brooklyn, Maryland

11. Yahoo provided the following email/chat messages found within the “apoc39” Yahoo account to which the user of “apoc39” was a party to: “i pay once kids there,” “have young girl now?” No further investigation was conducted into this specific user at the time Yahoo provided this information.

12. On August 19, 2020, Baltimore City detectives and members of the FBI Violent Crimes Against Children Task Force, including myself, executed a state search and seizure warrant at the residence located at 27 South Curley Street, Baltimore, Maryland 21224. Bickling was present and waived his Miranda rights and consented to an interview, in which I participated in, and which was audio and video recorded. Bickling advised his phone number was 443-739-3953 and his email address was sbick36@gmail.com. Bickling currently lives alone and has lived at his current residence for approximately one year. Bickling advised his current cell phone was an iPhone and that he has had the iPhone for three years. Bickling has owned his laptop for approximately eight years and no one else uses his laptop. Bickling advised that he had child pornography videos of children “probably between five and twelve” years old saved on his laptop. Initially Bickling stated he did not know how he acquired the videos because he had been drinking at the time and said it was over a year ago. Then Bickling advised that he visited child modeling websites and clicked on links and eventually found child pornography videos.

Bickling stated that he thought he saved twenty to thirty videos. Bickling initially stated he saved the videos once or twice over a two-month period and that he watched the videos approximately once a month, or less, and the last time he viewed the videos was possibly a couple of weeks prior to the interview when he was drinking. Bickling stated he paid approximately \$30 for access to the website and that he probably used his Visa credit card to pay for the access. Bickling denied watching child pornography with other people and denied trading the videos with others. Bickling stated his cell phone will not have child pornography on it. Bickling denied touching or taking sexual pictures of his daughter or any other child inappropriately. Bickling initially denied having any other digital items. When advised that several thumb drives were found he stated no child pornography would be found on them. After being advised that at least one thumb drive contained naked pictures of children, Bickling stated he hadn't looked at the thumb drives in awhile so he did not recall what was located on them.

13. Later the same day, during an interview with another investigator, Bickling admitted to communicating via Skype with people in the Philippines after first meeting them on adult Asian chat rooms. Bickling stated "I would send them money if they brought their child to get naked on Skype... but I've never physically touched a child." Bickling stated the female child was eight or nine years old. Bickling stated he did not ask the children to touch themselves or for anyone to touch them. Bickling requested the child to turn over, bend over on their hands and knees. Bickling admitted to masturbating while the child was on Skype and that it would last approximately five to ten minutes. Bickling paid \$50 via PayPal. Bickling stated he has done this eight to ten times over the past two years.

14. On August 19, 2020, at the end of the interview, Bickling wrote the following statement: "I believe beginning in early 2018 I began visiting a website called

fillipinawebcams.com which had live chat rooms with Asian women. After some visits to some rooms I heard children in the background and got the idea to ask the female performer to see if she would join me on Skype with her female child and I would pay her directly for a nude show with her daughter. I would join them on Skype video and usually pay \$50USD for her daughter to get naked and pose, mostly bent over from behind. I would masturbate until ejaculation in 5 to 10 minutes. In a two year span this occurred probably between 12-15 times is my best guess. I have not done this act since most likely October or early November of 2019. These acts were always done while I was drinking which was always excessive drinking.”

15. On January 22, 2021, Bickling was arrested pursuant to a criminal complaint and arrest warrant issued by the Honorable Thomas M. Digirolamo in violation of U.S.C. Title 18 Section 2422(b) (Attempted Online Coercion and Enticement of a Minor). Bickling has been detained since.

16. In October 2021, NCMEC advised that there were six Cybertipline Reports that appeared to be related to Steven Bickling. Five of the reports were received by NCMEC on November 20, 2013. They were submitted by ihrms@inhope.org¹. All five reports listed the reported URL as containing **beryydoq.com** as part of the URL address and stated “I accessed the reported URL and found a linking page titled, 'DVD !!! UNBELIEVABLE OFFER !!! DVD' which contains content that appears to be CHILD PORNOGRAPHY. I did not click on any links and cannot comment on content beyond this point.”

17. The registrar information listed in all five Cybertipline reports was:

Registrar: **GoDaddy.com, LLC**
Registrant Name: Steven Bickling
Registrant Street: 3514 Elliott

¹ INHOPE stands for the International Association of Internet Hotlines and IHRMS stands for INHOPE Report Management System. According to the INHOPES.org website, their mission “is to support and enable INHOPE hotlines in the rapid identification and removal of Child Sexual Abuse Material from the digital world.”

Registrant City: Baltimore
Registrant State/Province: Maryland
Registrant Postal Code: 21224
Registrant Country: United States
Admin Phone: 4437397509
Admin Email: bick36@gmail.com

18. The sixth report, **Cybertipline Report 2194409**, was received by NCMEC on November 21, 2013. The submitter was GoDaddy.com/Wild West Domains and the listed Incident Type² was “Apparent Child Pornography.” The report for **2194409** provided the following information regarding the GoDaddy Web Address (URL) being reported:

URL:	http://avza.berydoq.com
Email Address:	bick36@gmail.com ³
IP Address:	12.134.211.139 ⁴
Incident Time:	11/19/2013 20:55:00 UTC
Incident Type:	Child Pornography (possession, manufacture and distribution)

19. The report for **2194409** stated that there were four uploaded PDFs associated with the report. The report further stated that the “attached PDFs were only examples of many sites that were contained on this one hosting account.” In the Cybertipline Report, GoDaddy did not state whether they viewed the entire contents of the uploaded file. The uploaded files were provided with the Cybertipline report and have not been reviewed. The report also for **2194409** stated the following:

- On 11/19/2013 at 3:26:48 AM (-7 GMT) from IP address 12.134.211.139, our customer Steven Bickling purchased the domain name and hosting for **BERYDOQ.COM**
- Customer Account Billing Information: Steven Bickling, 3514 Elliott, Baltimore, MD 21224, Phone: 4437397509, bick36@gmail.com, Paid: Credit Card (VISA)

² NCMEC Incident Type is based on NCMEC’s review of the information OR a “Hash Match” of one or more uploaded files.

³ A subpoena was sent to Google for the email address bick36@gmail.com. The account was opened in November 2010 and was in the name Kevin Bick. No recent login IPs were provided by Google.

⁴ The IP address resolved back to AT&T and geolocated to the Washington, D.C. area. In 2013, NCMEC forwarded Cybertipline report 2194409 to the Virginia State Police. It is unknown at this time if any further investigation was conducted. An attempt to contact Virginia State Police has been made with negative results.

- The ip address listed was found to be uploading the child abuse content files onto the hosting account.
- All of the content located within the directories and on the various sites were all of the child exploitive nature.

20. On February 23, 2022, NCMEC provided FBI Baltimore the associated files of **Cybertipline report 2194409** via a .zip file. The associated files have not been viewed. The files were saved on a SanDisk 64GB thumb drive (SN150625268B), which is secured and in the custody of the Federal Bureau of Investigation, located at 801 International Drive, Linthicum, Maryland.

21. In February 2022, an email was sent to GoDaddy.com asking if they would still have the information associated with **Cybertipline report 2194409**. GoDaddy.com's response was "We retain information regarding Cybertipline reports in perpetuity."

22. On February 16, 2022, a real property search through the Maryland Department of Assessments and Taxation revealed that 3514 Elliott Street, Baltimore, MD 21224, the address listed in the Cybertipline reports as the registrar/customer address, was transferred to Steven Bickling in 2006, and that 3514 Elliott Street, Baltimore, MD 21224 was transferred to Bickling's ex-wife in 2016.

SUMMARY

23. Based on my training and experience and the fact set forth above, I believe that the user of the TARGET LOCATIONS displays characteristics common to individuals who have a sexual interest in children, and who access with the intent to view and/or, possess, collect, receive, produce, and distribute child pornography as discussed in paragraphs 6 and 7 above.

24. Based on my training, knowledge and experience, individuals who have a sexual interest in children and who produce, distribute, receive and possess child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private

environment. These collections are often maintained for many years – even decades. These individuals go to great lengths to conceal and protect their collection from discovery, theft, and damage. Individuals who collect child pornography prefer not to be without their child pornography for any prolonged time period and therefore they tend to keep their collection where they can easily access it such as in their residence, vehicles and place of employment, as well as on their person. Individuals who collect child pornography also tend to keep their collection on multiple devices, many of which are portable such as a smartphone, laptop computer, and external storage devices, such as flash drives, external hard drives, and other storage media. In my investigative experience, as well as the documented experience of other investigators, these devices are often kept in the individuals' homes, vehicles, place of employment and on their person.

25. Based on these characteristics, I respectfully submit there is probable cause that the TARGET LOCATIONS contains evidence (1) of production, online coercion and enticement of a minor, distribution, receipt, and/or possession of child pornography, and (2) are relevant to determine the ownership and control of the TARGET LOCATIONS. Based on my training and experience, such information may constitute evidence of the TARGET OFFENSES because the information can be used to identify the account's user or users.

CONCLUSION

26. Based on the foregoing information, I have probable cause to believe that contraband, evidence, fruits, and instrumentalities of the TARGET OFFENSES as set forth herein and in Attachments B1 and B2 is currently contained in the TARGET LOCATIONS, more fully described in Attachments A1 and A2. I therefore respectfully request that a search warrant be issued authorizing the search of the account described in Attachments A1 and A2, for the items

described in Attachments B1 and B2, and authorizing the seizure and examination of any such items found therein.

Rachel S Corn
Special Agent Rachel S. Corn
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and Fed. R. Crim. P. 41(d)(3) this 24th day of February, 2022.

A. David Copperthite
HONORABLE A. DAVID COPPERTHITE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A1

ITEMS TO BE SEARCHED

Associated files of Cybertipline Report 2194409 that were forwarded to the National Center for Missing and Exploited Children (NCMEC) by GoDaddy.com/Wild West Domains, which are stored on a SanDisk 64GB thumb drive (SN150625268B) currently in the custody of the Federal Bureau of Investigation, located at 801 International Drive, Linthicum, Maryland.

ATTACHMENT A2 – GoDaddy.com, LLC

This warrant applies to information associated with the following:

- Web Site/URL: <http://avza.berydoq.com> to include the Sub-Domain Names set up on BERYDOQ.COM: avza.berydoq.com, blzy.berydoq.com, cuyo.berydoq.com, dalj.berydoq.com;
- Customer Account: Steven Bickling, 3514 Elliott, Baltimore, MD 21224
Phone: 4437397509, bick36@gmail.com;

that are stored at premises owned, maintained, controlled, or operated by GoDaddy.com, LLC, a business with offices located at 2155 E. GoDaddy Way, Tempe, Arizona 85284.

ATTACHMENT B1

LIST OF ITEMS TO BE SEIZED

Any and all files containing a visual depiction of a minor, to include images and videos of children engaged in sexually explicit conduct as described in 18 U.S.C. § 2256, nude pictures, and modeling. Additionally, any communication, information, pictures, videos or documentation that identifies the user of the account or that indicates a sexual interest in children.

ATTACHMENT B2 – GoDaddy.com LLC

I. Files and Accounts to be produced by GoDaddy.com LLC between November 19, 2013, to the present.

To the extent that the information described in Attachment A2 is within the possession, custody, or control of GoDaddy.com LLC including any messages, emails, records, files, logs, images, videos, or information that have been deleted but are still available to GoDaddy.com, GoDaddy.com is required to disclose the following information to the government for each account or identifier listed in Attachment A2:

- a. Any and all content associated with GoDaddy.com **Cybertipline report 2194409**;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, email addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All information automatically recorded by GoDaddy from a user's Device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to connecting to the website, all information searched for on the website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;
- d. The types of services utilized by the user;
- e. All files and records or other information stored by an individual using the account, including all images, videos, documents and other files uploaded, downloaded or accessed using GoDaddy's service, including all available metadata concerning these files;
- f. All records pertaining to communications between GoDaddy and any person regarding the account, including contacts with support services, any complaints, and records of actions taken;
- g. The contents of all private messages and attachments stored in the accounts described in Attachment A2, including copies of messages sent to and from the account, draft messages, the source and destination accounts associated with each message, the date and time at which each message was sent, and the size and length of each message;
- h. The contents of the user's profile to include uploaded text, posts, images, video, quotes, or links to their account;

i. Records of session times and durations and IP addresses associated with each of these sessions for every user in each folder in this account;

j. The contents of any private or public blogs;

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the accounts described in Attachment A2 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2251(a), 2422(b), 2252A(a)(2), and 2252A(a)(5)(B), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Images depicting the interior or exterior of residences, public establishments, and vehicles;

5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

6. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

7. Evidence of the times the account or identifier listed on Attachment A2 was used;

8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A2 and other associated accounts;

10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

b. All existing printouts from original storage which concern the categories identified in subsection II.A; and

- c. All “address books” or other lists of contacts.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.